

GOVERNMENT OF ANDHRA PRADESH
ABSTRACT

ITE&C Department - Standards for new e-Governance applications development and systems integration, Data hosting, Data Access, Mobile applications, Social media engagement etc., - instructions to all departments - Reg.

INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS (eGov)
DEPARTMENT

G.O.Ms.No.3

Date:08.07.2020

Read:-

G.O.Rt.No.547 of General Administration (Cabinet) Department, Dated: 13-03-2020

ORDER:

Whereas e-Government (or electronic government) is the application of information and communication technologies to government procedures and functions to increase efficiency and enable effective citizens participation, Digital transformation entails digitization of the data and processes in e-Government, which include development of online portals for applications, mobile data services and engagement with social media for delivery of e-public services.

2. Various Government departments in Andhra Pradesh have taken up several initiatives under Information Technology (IT) and mobile applications to achieve the goals of e-Government and digital transformation. To achieve efficiency and optimal results, there is a need to follow uniform procedures, standards, and best practices. It has been observed that several departments are implementing e-Government and digital transformation projects without following common standards and protocols.

3. Vide GO read above, the Secretaries, Heads of Departments, Corporations and Autonomous Organizations have been directed that, all existing and new software application development, application hosting, Data sharing and Database accessing etc, shall conform to the standards and guidelines prescribed by Information Technology Electronics & Communications Department. Further, the Finance Department has been directed to ensure that all Secretaries, Heads of Departments, Corporations and Autonomous Organizations shall obtain the concurrence of Information Technology Electronics & Communications Department, regarding adherence to such prescribed Standards and Guidelines before approving any IT related expenditure.

4. Accordingly, common standards, guidelines and compliance matrices pertaining to the following IT initiatives are hereby prescribed for compliance by all Departments, Corporations and Autonomous Organizations.

P.T.O

::2::

- a. Software development for a new e-Government application, and software and systems integration(see part I)
- b. Data hosting (see part II)
- c. Data sharing and database access (see part III)
- d. Web site development (see part IV)
- e. Mobile applications development (see part V)
- f. Social media accounts and related engagement (see part VI)

5. The compliance matrices shall be authenticated by the Secretary of the department concerned for each of the activities listed above and circulate through e-Office to the Information Technology Electronics & Communications Department for technical concurrence. The detailed guidelines pertaining to the above are listed in the website of Information Technology Electronics & Communications Department (www.apit.ap.gov.in) along with useful links to relevant pages.

6. Since the field of e-Government, digital transformation and Information Technology in general, is constantly emerging with new standards and protocols, Information Technology Electronics & Communications department would update the existing standards and guidelines from time to time and list the same in the website of the Information Technology Electronics & Communications department. All the Secretaries are requested to keep abreast with such updates and ensure compliance of the same.

(BY ORDER AND IN THE NAME OF GOVERNOR OF ANDHRA PRADESH)

KONA SASIDHAR
PRINCIPAL SECRETARY TO GOVERNMENT

To

All Departments of Secretariat

All Heads of Departments

All Corporations/Autonomous organizations (through HoDs)

The Prl.Secretary to Govt., Finance Department.

IT Advisors

The PAO / DTO

Copy to:

The Spl. Secretary to Hon'ble Chief Minister

The OSD to Hon'ble Minister, IT

The P.S to Chief Secretary / Prl. Secretary (Political)

The P.S to Prl. Secretary to Govt., ITE&C Department

//FORWARDED::BY ORDER//

SECTION OFFICER

Part I

Standards for (1) software development for a new e-Government application, and (2) Software and systems integration of existing applications

The following compliance matrix captures the details of the e-Government project with reference to (1) software development for a new e-Government application, and (2) software and systems integration for existing e-Government projects. This compliance matrix shall be filled-in by the Secretary to Government for each of the e-Government projects undertaken in their department and currently in usage and send the same to ITE&C Department for technical concurrence.

S.No	Standards	Response of the Department w.r.t compliance of each standard prescribed
I. Features of the Application (See Note I in Annexure)		
1.	Title of e-Government Application	
2.	Purpose of the Application	
3.	Indicate:	
	<i>a) Start date of the project:</i>	
	<i>b) Date of completion of user acceptance testing (UAT) of the project:</i>	
	<i>c) Date on which security audit certification was obtained (see part IV):</i>	
	<i>d) Date on which SSL/TLS certification was obtained (see part IV):</i>	
	<i>e) Date of go-live of the project:</i>	
	<i>f) Period of Maintenance of the project (from mm/yyyy to mm/yyyy)</i>	
4.	Does the ownership of source code of the e-Government application rest with the department?	
5.	Does the Intellectual Property Rights of the e-Government application rest with the department?	
6.	Does this application use proprietary, licensed products?	
7.	If the response to (6) is yes, has permission been sought for the use of licensed products?	
8.	What is the size of the e-Government application? • Indicate whether Small/Moderate/Complex • Indicate size of the application in	

	MB/GB units	
9.	Time taken for (in working days):	
	<i>a) Requirements gathering</i>	
	<i>b) Software development and coding</i>	
	<i>c) Testing</i>	
10.	Cost incurred for requirements gathering, software coding, and testing activities, in Rs. Lakhs	
11.	Indicate the cost incurred for maintenance per annum, in Rs. Lakhs.	
12.	Whether developed by in-house team or outsourced to IT vendor?	
13.	If outsourced to IT vendor, indicate the following details:	
	<i>a) Name and address of the IT vendor</i>	
	<i>b) Capability Maturity Model Integration (CMMI), a process level improvement training and appraisal framework, defines 5 maturity levels for IT firms in software development: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. As a standard, the IT vendor must have been appraised a minimum of CMMI level of 3 and above.[1]</i>	
	<i>Indicate the CMMI level of the IT vendor with details.</i>	
	<i>c) Whether IT Vendor complied with ISO (International Standards for Organizations) 27001?</i>	
	<i>d) Contract period:</i> <i>For software development (from mm/yyyy to mm/yyyy)</i> <i>For maintenance (from mm/yyyy to mm/yyyy)</i>	
	<i>e) The IT vendor must be empanelled by APTS (or) the Government of India (or) selected through competitive bidding process. Is the IT vendor empanelled or selected through open bidding process? Provide details</i>	

	f) Has the IT vendor been blacklisted or penalized by the Government of AP or Government of India or any other Government/s in the past three years? Provide details.	
II. Coding (see Note II in Annexure)		
14	Date of receipt of the business requirement specification (BRS) by the IT vendor or departmental IT team:	
15	Date of finalization of the software requirement specification (SRS) by the department and the IT vendor or departmental IT team:	
16	Date of finalization of the functional requirement specification (FRS) by the department and the IT vendor or departmental IT team:	
17	As a best practice, Globals must not be used in a software application. Have globals been used in this e-Government application? If yes, provide justification.	
18	Method/procedure/function should not exceed 25 lines of code, as a best practice. Does this application contain method/procedure with more than 25 lines of code?	
19	Methods / procedures may not contain more than five arguments, as this will ensure minimal algorithmic complexity. Does arguments for methods / procedures in this application exceed five arguments?	
20	While there is no restriction on the total lines of code for the application, component files may contain a maximum of 1000 lines of code to prevent coding complexity. Do any of the program files for this application exceed 1000 lines of code?	
21	Numbers and strings may not be hardcoded, and constants must be declared in the beginning. Are numbers and strings hardcoded in this application?	
22	Error messages should be generic to the end users, and detailed messages may be made a part of application logging. How are error messages handled?	
23	Use of 2-level folder hierarchies, with up to 10 folders in the root folder is optimal. Comment on hierarchies in this application.	

24	Sensitive information like database connection, and API authorization keys may not be exposed as part of “View Page Source”. Is this practice followed?	
25	Database Schema Design must be reviewed and published with entity relationship (ER) diagrams to understand the relations between database tables and data types. Has the database schema design published for this application?	
26	Are unused variables or methods removed from this application?	
27	Are the logs maintained when fields with financial impact are modified?	
28	Is the default access “deny”?	
29	Is the principle of least privilege adhered to?	
30	Sanitizing data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components is a best practice. Has this been complied with?	
31	Is the application’s internet protocol (IP) address white listed?	
32	Are the API-receiving entities white listed?	
33	Untrusted data sources is a source for a majority of software vulnerabilities. Are the data sources used in this application https – authenticated?	
III. Testing (See Note III in Annexure)		
34	Systems requirement specification (SRS) is the mother document for the application, which would have been specified during requirements gathering. Does the testing document and cases align with the final version of the SRS?	
35.	Please mention the time taken (in working days) for the testing phase:	
	<i>a) Phase (i) to (v)</i>	
	<i>b) Phase (vi) and (vii)</i>	
	<i>c) Phase (viii)</i>	
36.	<i>d) Phase (ix)</i>	
	As a standard interface, text must be left aligned and numbers right aligned. Currency must have two decimal places and right aligned. Is this interface followed?	
37	Headers of grids must be meaningful, and	

	easily understandable to the user. How are headers named in this application?	
38	Are values in the drop down list in alphabetical order?	
39	Are Reset / Clear button provided to reset or clear the values?	
40	Messages must be displayed in standard format. Are success messages displayed in GREEN and Error/Failure message in RED?	
41	Sensitive information like Aadhar Number, Phone Number, Bank Account Numbers should be masked. Is this practice followed?	
Go-live		
42	Data and documentation (pertaining to problem reports, software deviations and exceptions) of the Software Development Life Cycle (SDLC) must be maintained with proper time and date stamps, and deposited with the department before go-live. Has this documentation reached the department?	
43	Did the application pass the user acceptance testing (UAT)?	
44	Traceability matrix must be deposited with the department before go-live. Has this matrix been received by the department?	
45	Is the software application virus checked and corruption free? Any of the top 5 antivirus software ranked by PC magazine (https://in.pcmag.com/) may be used.	
IV. Cyber Security (See Note IV in Annexure)		
46	Is the application Security Audited with reference to the following controls? Indicate (Yes/No) against each control	
	<i>a) Configuration management</i>	
	<i>b) Secure transmission</i>	
	<i>c) Authentication</i>	
	<i>d) Sessions management</i>	
	<i>e) Tests for authorization</i>	
	<i>f) Data validation</i>	
	<i>g) Denial of service</i>	
	<i>h) Business logic</i>	
	<i>i) Cryptography</i>	
	<i>j) Risk functionalities for file uploads and card payments</i>	
	<i>k) HTML 5 compliance</i>	
47.	Has the Security Audit Certificate been issued by	

	the CERT-In empanelled vendor/APTS before hosting in production environment? If yes, the audit clearance certificate to be uploaded in the department's portal/website, and a copy be sent to ITE&C Department. (Para 7 of GO Ms. No. 4 ITE&C (Infra) Department dated 10-01-2019).	
48	The SSL/TLS certification should be at the minimum organization-validated, and for a single-domain. Does the application portal have SSL / TLS certification? If yes, the audit clearance certificate to be uploaded in the department's portal, and a copy be sent to ITE&C Department. (Para 4.1 controls (PROTECT-89) of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019).	
49	As a best practice, the e-Government application can go-live only after: (i)obtaining security audit certificate by a CERT-In empanelled vendor / APTS (ii) obtaining SSL /TLS certification. Has this been complied with?	
50	Security audit must be done every twelve months. When was the last Security Audit conducted? (Para 4.1 controls (IDENTIFY-7) of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019)	
51	If your website/application is integrated with any 3rd party Applications or using any Application Program Interface (APIs) for external communication, a standard practice is to use an encrypted channel. Is this being followed? Para 4.1 controls (PROTECT-76) of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019	
52	Is the Infrastructure/Network Audit done for the hosting location? (Para-4 of Go.MS 4 ITE&C (Infra) Department dated 10-01-2019)	
53	Is Vulnerability assessment and Penetration test (VA&PT) done for IT Assets [which include servers, networking medium, and components]? (Para-4 of Go.MS 4 ITE&C (Infra) Department dated 10-01-2019)	
54	Has Server Hardening been done? (Para-4 of Go.MS 4 ITE&C (Infra) Department dated 10-01-2019); Please indicate the date of previous hardening instances, including the latest instance.	

55	If SSL is installed, the standard is to include TLS version 1.2 as a minimum. Please indicate the TLS version presently in use (Page-41 of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019).	
56	The minimum encryption standard is Advanced Encryption Standard (AES) 128 -bit and higher. What is the encryption used for internal communication (DB/Authentication/ Fileservers)? (Page-40,41 of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019)	
57	As a standard, the application must not permit simultaneous logins. Indicate whether the application permits simultaneous logins (Page-37 of GO Ms. No.18 ITE&C (Infra) Department dated 6-03-2019)?	
58	Whether Department on-boarded the IT Assets to Andhra Pradesh Cyber Security Operations Centre (APCSOC) to enable monitoring and to identify the possible cyber threats (Para 5 of GO Ms. No. 6 ITE&C (Infra) Department dated 25-01-2019)	
59	For the IT Assets hosted at Department's premise, whether redundant connectivity from Department site to APCSOC Primary and Secondary Data Centres is established for Log collection and Monitoring or not? (Para 6 of GO Ms. No. 6 ITE&C (Infra) Department dated 25-01-2019).	
60	Whether the department identified a Single Point of Contact (SPoC), who shall be responsible for Security Compliance of the Department and, has the SPoC details communicated to APTS/APCSOC. (Para 7 of GO M.s No. 6 ITE&C (Infra) Department dated 25-01-2019)	
61	Has the details of the Critical Information Infrastructure (CII) updated in the website (URL:https://ITAssets.apt.gov.in) ? – para 5 of GO.MS.No.4 of ITE&C (Infra) Department dated 10-01-2019.	
62	Has the details of the active assets updated in the website (URL:https://ITAssets.apt.gov.in)? CII has to undergo security audit as a default standard. Has the CII been security audited? Indicate the date of the security audit? Para 6 of	

	GO Ms. No. 4 of ITE&C (Infra) Department dated 10-01-2019.	
63	Whether the department classified the IT assets based on the following classification: i. High Critical IT Assets - once in 3 months ii. Medium Critical IT Assets - once in 6 months iii. Low Critical IT Assets - once in a year Para 6(c) of GO Ms. No. 4 of ITE&C (Infra) Department dated 10-01-2019.	

Date:

(Signature)
Secretary to Government
----- Department

Part II

Standards for Data Hosting

This compliance matrix shall be filled-in by the Secretary of the Department for each of the e-Government projects undertaken in their departments and currently in usage and which have data hosting requirements, and send the same to ITE&C Department for technical concurrence.

S.No	Guideline	Response of the Department w.r.t compliance of each standard prescribed
1.	Hosting ID of the data hosting application	
2.	As a standard practice, government applications must be hosted in the AP state data centre (APSDC)? Is the Application hosted at AP State Data Centre?	
3.	If Application is hosted outside APSDC, mention the details of the data hosting vendor as follows:	
	a) Name of the outsourced data hosting centre	
	b) Location	
	c) Dedicated server or Virtual Machine or Cloud	
	d) Contract period details	
	e) Status of Infrastructure Hardening (Server/Network)	
	f) Capability Maturity Model Integration (CMMI), a process level improvement training and appraisal framework, defines 5 maturity levels for IT firms in software development: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. As a standard, the IT vendor must have been appraised a minimum of CMMI level of 3 and above. Indicate the CMMI level of the data hosting vendor.	
	g) Whether the data hosting vendor complied with ISO (International Standards for Organisations) 27001?	
	h) As a standard, the data hosting vendor must be empanelled by APTS or the Government of India or selected through competitive open bidding process. Is the vendor empanelled or selected through open bidding process? Provide details	

	<i>i) Has the data hosting vendor been blacklisted or penalized by the Government of AP or Government of India or any other Government/s in the past three years? Provide details.</i>	
4.	Does the data hosting vendor Helpdesk & technical support on 24x7x365 basis?	
5.	Does the data hosting vendor have multi-tier security infrastructure, firewall and intrusion prevention systems?	
6.	Does the data hosting vendor have a Disaster Recovery (DR) Centre in a geographically distant location?	
7.	The data hosting vendor must possess redundant server infrastructure and performs regular backup of the website to ensure high availability in an efficient and secure manner on a 24x7 basis. Is this being adhered to?	
8.	Specify the cost incurred per month for data hosting (in Rs. Lakhs)	

Note: If Application is hosted outside APSDC, department has to fill-in columns 3, 4, 5, 6, 7 and 8.

Date:

Signature

Secretary to Government
----- Department

Part III

Standards for Data Sharing and Data Base Access

The following compliance matrix shall be filled-in by the Secretary of the Department for instances of data share, and database management protocols related to the e-Government projects undertaken in their department and currently in usage and send the same to ITE&C Department for technical concurrence.

S.No	Standards	Response of the Department w.r.t compliance of each standard prescribed
1.	Title of eGovernment Application for which the data base access/ sharing was done	
2.	Purpose of the data share/ access given	
3	Data access and share between source and requesting departments must be effected only through application programming interface (API), after securing approval in Form A (attached to this GO). Please provide details of previous shares of data till date in the format shown in Table 3 in Annexure	
4.	Granular access rights for removable devices and USBs within the department must be implemented to secure the data and prevent misuse. Provide details of employees who are given access rights for USBs and removable devices in the department.	
5.	Access to workstations / desktops access should be controlled to prevent misuse. Please indicate the restrictions imposed on access to workstations and desktops in the department.	
6.	Sensitive data and financial information which are shared, and in word-, pdf-reports must be password protected. Is this practice followed?	
7.	Email archiving prevents destruction of critical data. Indicate the details of email archives in the department.	
8	Data files must not be uploaded over http, webmail, file transfer protocol (FTP), and peer-to-peer (P2P) network, which are unsecured. Have any data files uploaded over such insecure sites in the past? If yes, provide details of all these uploads in the format shown in Table 4 in	

	Annexure	
9	In alignment with the standard human layer -8 identity-based network security, provide details of employees who are authorized to access data files, and work stations in the department. This shall ensure responsibility for data flow and control[2].	
10	Develops environment, production environment, and testing environment must be maintained separately with access controls. Is this being followed?	
11	Database access controls are required for securing data. As a standard, rights access must be implemented. Provide the following details: <i>a) Data Base Access rights have to be vested with a data base administrator/s, who must possess the appropriate qualification and certification. Provide details of the data base administrator/s:</i> <i>Data Base Administrator 1:</i> <i>Name:</i> <i>Designation:</i> <i>Organization /Department:</i> <i>Qualification:</i> <i>Relevant work experience:</i> <i>Certification:</i> <i>Official email id:</i> <i>Official phone no.:</i>	
	<i>Data Base Administrator 2:</i> <i>Name:</i> <i>Designation:</i> <i>Organization /Department:</i>	

<i>Qualification:</i> <i>Relevant work experience:</i> <i>Certification:</i> <i>Official email id:</i> <i>Official phone no.:</i>	
<i>Data Base Administrator 3:</i> <i>Name:</i> <i>Designation:</i> <i>Organization /Department:</i> <i>Qualification:</i> <i>Relevant work experience:</i> <i>Certification:</i> <i>Official email id</i> <i>Official phone no.:</i>	
<i>b) Is the Load testing done on the data base?</i> <i>Provide a date-and-time stamped report of the load testing.</i>	
<i>c) Has concurrency of users on the data base checked? Provide a date-and-time stamped report of the concurrency testing.</i>	

Date:

Signature
Secretary to Government
 ----- **Department**

Part IV

Standards for Web site development

This compliance matrix shall be filled-in by the Secretary of the Department for each of the website applications and hosting undertaken in their department and currently in usage and send the same to ITE&C Department for technical concurrence.

S.No	Standards	Response of the department w.r.t compliance of each standard prescribed
1. Government Identifiers		
1	Title of the e-Government Website application	
2	Purpose of the Website application	
3	Association to Government of AP must be indicated by the use of Emblem/Logo, prominently displayed (Emblem issued by Government of Andhra Pradesh vide Government Order no. 2, General Administration Department (PUA) dt:14.11.2018) the homepage of the website	
4	Ownership information is displayed on the homepage and on all important entry pages of the website.	
5	Complete and self-explanatory title of the homepage (appearing on the top bar of the browser) is provided.	
6	Website is registered under 'gov.in' or 'nic.in' domain	
7	Website provides a prominent link to the 'National Portal' (the national portal is the corresponding Government of India website with reference to the department) [3] from the Home Page and Pages belonging to National Portal load in new browser window.	
2. Building Confidence		
8	Website has a copyright policy, prominently displayed on the homepage	
9	Due permissions have been obtained for publishing any content protected by copyright.	
10	Source of all documents, whether reproduced in part or full, is mentioned	
11	Website has a comprehensive hyper-linking Policy	

12	Clear indications are given when a link leads out to a non government website	
13	The mechanism is in place to check the accuracy of Hyperlinked Content	
14	Mechanism is in place to check that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	
15	Website has a comprehensive Terms & Conditions statement, linked from all important pages	
16	Terms& Conditions statement disclaims responsibility of the content sourced /linked from a non Government website and clearly indicates whether information available on the site can be used for legal purposes or not.	
17	Website has a Privacy Policy linked from all the relevant pages	
18	All electronic financial transactions are handled through secure means	
3. Scope of Content: Primary Content		
About us		
19	All information about the department useful for the citizen and other stakeholders is present in the 'About Us' section and mechanism is in place to keep the information up to date.	
Schemes		
20	The complete title of the scheme is reflected	
21	Website provides a complete description of the scheme along with the procedure for obtaining the associated benefits	
22	The validity of the scheme has been mentioned	
Services		
23	Self explanatory title of the service is published	
24	The website provides a complete description of the service along with the procedure to apply for / avail the same	
Forms		
25	The website provides the complete title of the form along with the purpose it is used for.	
26	Language of the Form (other than English) is mentioned clearly.	
Acts		

27	The complete title of the Act (as written in the official notification) is mentioned.	
Documents		
28	The complete title of the Document is mentioned on the website.	
29	The language of the Document (other than English) is mentioned clearly.	
30	Validity of the Document has been mentioned.	
Circulars and Notifications		
31	The official title of the Circular/Notification is mentioned	
32	Validity of the Circular/Notification is mentioned	
Tenders and Recruitment		
33	Mechanism is in place to ensure that all Tender/Recruitment Notices issued by the Department are published on the website	
34	Website provides a complete description of the Tender/Recruitment notice along with the procedure to apply for the same	
35	Mechanism is in place to ensure that information on old /irrelevant tender/recruitment notice is removed or moved into the archive section	
News and Press Releases		
36	News/Press releases are displayed along with the date and these are organized as per the archival policy of the website	
Contact Us		
37	Website has a "Contact Us" page, linked from the home page and all relevant places in the website	
38	The complete contact details of important functionaries in the department are given in the 'Contact Us' section.	
39	Only the official contact details (email ids and contact numbers) of all the officers concerned are to be published in the Contact Us section	
Presence of the National Portal		
40	Mechanism is in place to ensure that all the citizen services, forms, documents and schemes are registered with the respective repositories of the national portal	

Scope of Content: Secondary content		
41	Mechanism is in place to ensure that all outdated announcements are removed from the website or moved to archive.	
42	All discussion forums on website are moderated	
43	For every related link, the complete Uniform Resource Locator (URL) of the homepage / concerned webpage is provided.	
Scope of Content: Tertiary Content		
44	Feedback is collected through online forms and mechanism is in place to ensure timely response to feed back /queries received through the website.	
45	The website has a readily available help section	
46	Complete information including title, size (playing time for audio/video), format, usage instructions and plugin to view the file is provided for downloadable material including documents	
47	Mechanism is in place to ensure that all downloadable material is free from virus	
48	Minimum Content as prescribed in the guidelines is present on the homepage	
49	Subsequent pages of the website have the minimum content as prescribed in the guidelines	
50	Website is free from offensive/discriminatory language	
4. Quality of Content		
51	Content is compiled and packaged with citizen orientation	
52	The department has a content contribution, moderation and approval policy (CMAP) for the website	
	As a best practice, creation and management of digital content must be handled through a content management system (CMS) like Wordpress. Is this followed?	
53	Homepage and every important entry page of website displays the last updated/ reviewed date	
54	Department has a content review policy (CRP) for the website	

55	All documents/reports have a time stamp at least on the main page	
56	The departments have a clearly laid out content archival policy (CAP) for the website	
57	Clear and simple language has been used throughout the website	
58	The language is free from spelling and grammatical errors.	
59	Whenever there is a change in the language of a website it has been clearly indicated	
60	Consistency in nomenclature is maintained across the website	
61	All information, which is of direct importance to the citizen, is accessible from the homepage	
62	Information structure and relationship is preserved in all presentation styles	
63	The meaningful reading sequence is preserved in all presentation styles	
64	Documents/pages in multiple languages are updated simultaneously	
5. User Interface (UI) and User Experience (UX) Design		
65	Visual/textual identity elements highlighting the Government's ownership of the website are prominently placed on the page	
66	A consistent page layout has been maintained throughout the website	
67	National identity symbols like flag, national emblem, etc., are in a proper ratio and colour	
Language Print		
68	<i>a) Hindi/regional language fonts have been tested on popular browsers for any inconsistency (Loss of Layout).</i>	
	<i>b) Language option for website application to display in English and Telugu is clearly indicated.</i>	
69	Web pages allow resizing of text without the use of assistive technology.	
70	Text is readable both in electronic and print format and the page prints correctly on an A4 size paper	
71	There is adequate contrast between text and background colour	

72	All information conveyed with colour is also available without colour	
73	Alternate text is provided for non text elements (e.g images)	
74	Websites provide textual description of audio /video clips & multimedia presentation	
75	Caption have been provided for all important audio content	
76	Webpages do not contain any content that flashes for more than 3 times in a second.	
77	There is a mechanism for user to control scrolling, blinking content	
78	There is a mechanism for user to control (stop, pause)audio that starts automatically.	
79	All pages on website have link to the homepage	
80	The positioning and terminology used for navigation items and navigation scheme is consistent across the website	
81	There are no links to 'Under construction' pages	
82	Each page standalone entity in terms of ownership, navigation and context of content	
83	Webpages allow the user to bypass repeated blocks of content	
84	Website has either a "search" box or a link to a "search page" from every page of the website	
85	Website has an up-to-date site map that is linked to the homepage as well as to all important entry pages of the website	
86	If the site uses frames, each frame is properly titled	
87	Responsive Web design mode must be followed for designing the website (i.e) adjusts to phones, tablets, and desktops	
	<i>a) Does the website adopt the mobile-first approach? (i.e) involves designing a desktop site starting with the mobile version which is then adapted to larger screens?</i>	

	<i>b) Does the website design supports Lazy loading (i.e.) Load only the required elements to display where ever accessed?</i>	
6. Development		
88	Does the website use cascading style sheets to control layouts/styles	
89	Is the website readable even when styles sheets are switched off or not loaded	
90	Is the webpage usable even when scripts, applets etc., are turned off	
91	Are documents provided either in Hypertext Markup Language (HTML) or other accessible formats. Instructions/download details for viewing these formats are provided	
92	In content implemented using markup languages the elements have been used according to specification	
93	Labels have been provided when content requires input from the users	
94	Time limit for time dependent web functions can be adjusted by the user	
95	Instructions for operating / understanding content do not rely solely on characteristics like shape size, location, etc.,	
96	All input errors are flashed in text	
97	Functionality of content is operable through keyboard	
98	Focus is not trapped in any component while navigating through keyboard only	
99	Purpose of each link is clear to the user	
100	When any component receives focus it does not initiate change in context	
101	Change in the setting of a component does not change the context unless the user has been informed of the same	
102	Metadata for page like title, keywords, description and language is appropriately included	
103	Data tables have been provided with necessary tags/markup	
104	All components receive focus in an order that preserves the meaning/operation	
105	Role of all interface components can be programmatically determined	

106	The website has been tested on multiple browsers	
107	The website has cleared security audit by certified agency and has a security policy. Applications configured to send mail are enabled over Simple Mail Transfer Protocol (SMTP-AUTH)	
7. Website Hosting		
108	Websites are accessible to the intended audience in an efficient and secured manner on 24X7 basis	
109	The hosting Service Provider performs regular backup of the website	
110	Webhosting Service Provider provides help desk and technical support on 24x7 x365 basis.	
111	All possible security measures have been taken to prevent defacement/hacking of the website and the department has contingency plan in place for situations like these	
112	Is the security Audit done for this website application?	
113	Is the Secured Socket Layer (SSL)/Transport Layer Security (TLS) certificate in place for the website?	
8. Website Promotion		
114	Website ranks in the first 5 results on major search engines when searched with relevant keywords	
115	It has been ensured that advertisements/public messages issued by the concerned department prominently display the URL of the website	
9. Website Management		
116	Has the Department nominated a web information manager as defined in the guidelines	
117	The website has a website monitoring policy	
118	All policies and plans are approved by the Head of Department	
10. Cost incurred (in Rs. Lakhs per annum)		
119	For development	
120	For maintenance	
121	Whether developed by in-house team or outsourced to IT vendor?	

	If outsourced to IT vendor, indicate the following details:	
	a) <i>Name and address of the IT vendor</i>	
	b) <i>Capability Maturity Model Integration (CMMI), a process level improvement training and appraisal framework, defines 5 maturity levels for IT firms in in software development: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. As a standard, the IT vendor must have been appraised a minimum of CMMI level of 3 and above.[4]</i> <i>Indicate the CMMI level of the IT vendor details.</i>	
122	c) <i>Whether the Vendor complied with ISO (International Standards for Organizations) 27001?</i>	
	d) <i>Contract period:</i> <i>For software development (from mm/yyyy to mm/yyyy)</i> <i>For maintenance (from mm/yyyy to mm/yyyy)</i>	
	e) <i>Is the vendor empanelled or selected through bidding process? Provide details</i>	
	f) <i>Has the vendor been blacklisted or penalized by the Government of AP or Government of India or any other Government/s in the past three years? Provide details.</i>	
	g) <i>Time taken (in working days) for development of the application</i>	
	h) <i>Contract period</i>	
123	Indicate size of the application in MB/GB units	
124	Does the source code and Intellectual Property Rights of the website application rest with the department?	

Date:

Signature
Secretary to Government
----- Department

Part V

Standards for Mobile Application Development

The following compliance matrix shall be filled-in by the Secretary, of the Department for each of the mobile apps developed in their department and currently in usage and send the same to ITE&C Department for technical concurrence.

S.No	Standards	Response of the Department w.r.t compliance of each standard prescribed.
1. Accessibility Guidelines		
1.	Title of Mobile Application	
2.	Purpose of the Application	
3	Platform Accessibility features have been optimally used and they behave as intended	
4	Proper labels have been provided for all User Interface (UI) elements	
5	The role of a UI element is available so that assistive technology can report this either through speech or Braille.	
6	Hints have been provided for all active UI control elements	
7	The changes of the state of UI controls are dynamically updated and accurately available to the assistive technologies.	
8	Related UI elements have been grouped together.	
9	A non-interactive space of at least one point for iPhone Operating System (IOS) or 1 Density independent pixel (DP) for android has been provided between actionable UI elements.	
10	Touch targets are at least 9X9 millimeter regardless of screen size.	
11	Focus is always on the active UI control.	
12	When a UI control has context specific menu items, users are informed that such a menu is present and are able to activate those menu items.	

13	Content when envisaged using the screen reader gestures forms a meaningful sequence	
14	The app resizes its UI elements in accordance with device settings for text size.	
15	Color contrast ratio between foreground text for up to 18 point font and background is at least 4.5:1	
16	Color & shape is not the only means to communicate important information.	
17	Focus is changed only when the user activates a UI element that is designated for confirming an action such as the Submit button.	
18	Appropriate keyboard is invoked by the app depending on the type of field or the data that needs to be provided by the user.	
19	Apps is compatible with hardware keyboard.	
20	Gestures do not require 3 or more fingers to interact with UI elements.	
21	Session timeouts have been avoided. If a timeout cannot be avoided, then an option has been provided for users to extend the time limit before the timeout occurs.	
22	Captions have been provided for all audio content and subtitles /transcript have been provided for all video content that is accompanied by audio.	
23	For videos that do not have an audio equivalent, audio description for the video content that is crucial for blind users to understand the content has been provided.	
24	No content flashes more than 3 times in one second.	
2. General Guidelines		

25	Association to Government of AP is demonstrated by the use of Emblem/Logo, prominently displayed (Emblem issued by Government of Andhra Pradesh vide Government Order no. 2, General Administration Department (PUA) dt:14.11.2018) the homepage of the website	
26	Clear instructions on using the app have been provided	
27	Mobile app and Application Programming Interface (APIs) have been security audited by Cert-in empanelled vendors	
28	APIs have been hosted in secure data centres equipped with firewalls and other security features.	
29	Hosting service provider provides 24X7 access to Application Program Interfaces (APIs) and back end databases.	
30	Only the official contact details (email ids and contact no.s) of all the officers concerned are to be published in the Contact Us section.	
31	Does the source code and Intellectual Property Rights of the mobile application rest with the department?	
32	Cost incurred (in Rs. Lakhs)	
	a) For development	
	b) For maintenance	
	c) Whether developed by in-house team or outsourced to IT vendor?	
33	If outsourced to IT vendor, indicate the following details:	
	a) Name and address of the IT vendor	
	b) Capability Maturity Model Integration (CMMI), a process level improvement training and appraisal framework, defines 5 maturity levels for IT firms in software development: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. As a standard, the IT vendor	

	<i>must have been appraised a minimum of CMMI level of 3 and above.</i> <i>Indicate the CMMI level of the IT vendor details.</i>	
	<i>c) Whether the Vendor complied with ISO (International Standards for Organizations) 27001?</i>	
	<i>d) Contract period:</i> <i>For software development (from mm/yyyy to mm/yyyy)</i> <i>For maintenance (from mm/yyyy to mm/yyyy)</i>	
	<i>e) Is the vendor empanelled or selected through bidding process? Provide details</i>	
	<i>f) Has the vendor been blacklisted or penalized by the Government of AP or Government of India or any other Government/s in the past three years? Provide details.</i>	
	<i>g) Time taken (in working days) for development of the application</i>	
	<i>h) Contract period</i>	
34	Indicate size of the application in MB/GB units	

Date:

Signature
Secretary to Government
 ----- **Department**

Part VI

Standards for Social media accounts and related engagement

The compliance matrix captures the details of the e-Government project which has association with the social media activities undertaken in their departments. This compliance matrix shall be filled-in by the Secretary of the Department for each of the social media activity current in their department and send the same to ITE&C Department for technical concurrence.

S.No	Standards	Response of the department w.r.t compliance of each standard prescribed
1. Accessibility Guidelines		
1	<i>a) User Name of the social media handle</i>	
	<i>b) ID of the social Media handle</i>	
	<i>c) Purpose of the Social Media engagement.</i>	
	<i>d) Is a proper record of all login ids & passwords maintained?</i>	
2	<i>a) Has the consent of the Secretary to Government of the department been taken for creating the social media account ?</i>	
	<i>b) Social media must be posted through official email only which is linked to the social media. Has this been followed?</i>	
	<i>c) The user credentials of the social media account must be accessed by a permanent Government official, approved by the Secretary to Government of the concerned department. Has this been adhered to?</i>	
	<i>d) Name and designation of the permanent Government official designated to handle the</i>	

	<i>social media account</i>	
	<i>e) Whether any fake social media accounts identified so far?</i> <i>If 'yes' how many such accounts are identified and what action has been initiated?</i>	
	<i>f) Whether the success stories of the department published in the social media?</i> <i>If 'yes' please furnish the details of such stories along with the dates published so far.</i>	
	<i>g) Adverse comments and exceptions received by the department must be responded to, on a real-time basis, and no later than six hours. Is this adhered to?</i>	
3	Whether the resources roles and responsibilities are clearly marked out?	
4	Whether the platform permits others to add their own content? If so whether any moderation policy is published including copyright, rights to addition and deletion etc.?	
5	Are the records created by Service Providers maintained with appropriate tags?	
6	Whether any rules are established that all policy announcements will be undertaken simultaneously on traditional as well as social media?	
7	Whether the social media account establishes the organization's online identity to ensure ease of search on the internet?	
8	Whether the roles and responsibilities of the team responsible for creating, managing and responding on social media platforms have been clearly defined?	

9	Whether the Data retention policy is being followed for social media accounts same as other electronic and non-electronic channels	
10	Is the department's social media account verified by the social media service provider? (Should obtain a verification badge of authenticity by the social media service provider).	
11	Cost incurred (in Rs. Lakhs)	
12	Whether developed by in-house team or outsourced to IT vendor?	
13	If outsourced to IT vendor, indicate the following details:	
	<i>a) Name and address of the IT vendor</i>	
	<i>b) Capability Maturity Model Integration (CMMI), a process level improvement training and appraisal framework, defines 5 maturity levels for IT firms in software development: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. As a standard, the IT vendor must have been appraised a minimum of CMMI level of 3 and above.</i> <i>Indicate the CMMI level of the IT vendor with details</i>	
	<i>c) Whether the Vendor complied with ISO (International Standards for Organizations) 27001?</i>	

	<i>d) Is the vendor empanelled or selected through bidding process? Provide details</i>	
	<i>e) Has the vendor been blacklisted or penalized by the Government of AP or Government of India or any other Government/s in the past three years? Provide details.</i>	
	<i>f) Contract period</i>	
14	Indicate size of the application in MB/GB units	

Date:

Signature
Secretary to Government
 ----- **Department**

Compliance Report
(GO.Ms.No.3 ITE&C (eGov) Department dated 08-07-2020)

(To be authenticated by the Secretary to the Government of the concerned Department)

Name of the Department:

Name and details of the Head of the Department:

Single Point of Contact details (email and mobile):

1. It is hereby certified that, all e-Government initiatives undertaken by the department and which are currently in use have been developed adhering to the guidelines prescribed in G.O.Ms.No.3 ITE&C(eGov) Department Dated 08-07-2020.

2. The compliance matrix for the standards on for the following is enclosed:

- ☐ Standards for(1) software development for a new e-Government application, and (2) software and systems integration of existing applications
- ☐ Data hosting
- ☐ Data Sharing
- ☐ Web site development
- ☐ Mobile applications development
- ☐ Social media accounts and related engagement

Date:

Signature

Secretary to Government

-----Department

Annexure

(GO.Ms.No.3 ITE&C (eGov) Department dated 08-07-2020)

Note I:

A. Classification of e-Government applications

e-Government applications shall be classified into small, medium and complex based on the following criteria, as shown in Table 1.

Table 1: Criteria for classification of e-Government applications

S.No	Size of the Software application	Levels of approval within the Government	Time taken for software development, working days	Team size to deliver output for one working day
1	Small	≤ 2	T0+7 to T0+10	One senior programmer, one junior programmer, one database analyst, and one tester.
2	Medium	>2 and ≤ 5	T0+11 to T0+60	One senior programmer, one junior programmer, one database analyst, and one tester.
3	Complex	>5	$> T0+60$	Two senior programmers, two junior programmer, one database analyst, and a testing team (comprising of one tester and one team member).

Notes:

- 1. 'T0' is defined as that working day when the software development team (from in-house or from service provider) finalizes the functional requirements of the e-Government application, in writing or email, by the concerned Head of Department (HoD).*
- 2. The criterion for the classification of e-government projects must be based either on the levels of approval within the government or the time taken for software development. For example, a project that has four levels of approval, but takes more than 60 working days for software development is classified as a complex project.*
- 3. Software development includes activities for requirements gathering, coding, testing, integration activities necessary for going live, and does not include maintenance activities.*

B. Documentation

Documentation is an important aspect of the project, and essential from requirement analysis up to project closure and updating the same is the key for project development and maintenance. This need to be updated regularly during the software development lifecycle (SDLC) to reflect the present status and shared with the concerned Government Department.

C. Source Code

If the department has outsourced the software development of the e-Government project to a service provider (usually IT vendors from the private sector), the source code of the e-Government project must be handed over to the department owning the project with proper comments and details, after the project closure. The source code, by default, must be owned by the government department to prevent the service provider from using the same or a customized version of this code for future profits. The source code should be delivered periodically to the requesting department during the various stages of the SDLC and the support phase with proper comments, and conventional time and date stamps.

D. Intellectual Property Rights (IPR)

The IPR of any software development, support and customization done for various projects for any department shall be exclusively with the Government of AP only. The service providers and IT vendors are prohibited from using the source code, with or without customization, in other similar digital transformation projects, for any state within or outside India, and the Government of India.

E. Use of open source products

To ensure open exchange, collaboration, rapid prototyping, meritocracy, and community involvement, the participating departments may use open source software for their applications as the default option. For use of proprietary software resources in e-government projects, IT vendors, service providers, or government departments must seek specific approval of the principal secretary, ITEC department with proper justification.

Note II. Standards for coding

The software development lifecycle (SDLC) comprises of the following distinct sequence of stages for developing a specific software product:

- i. communication,
- ii. requirements gathering,
- iii. feasibility study,
- iv. systems analysis,
- v. software design,
- vi. coding,
- vii. testing,
- viii. integration,
- ix. implementation,
- x. operations and maintenance, and
- xi. disposition.

Considerable financial and manpower resources have to be incurred for gathering requirements from the concerned government departments, coding, testing, and integration of an e-government software application.

While being agnostic to programming languages, these standards prescribed, help in optimizing CPU and memory resources.

Note III: Standards for Testing

Software development must be followed by rigorous testing, which have distinct phases, as shown in Table 2, which must be followed.

Table 2: Testing phases for software application and timelines

Sl. No.	Phase	Time Lines (in working days) for Each Phase of Testing		
		For Small Applications	For Medium Applications	For Complex Applications
I	Requirement Analysis	1	2	2
ii	Test Planning			2
iii	Test Scenarios Preparation			1
iv	Test Cases Development		1	2
v	Test Script Development (Automation)		3	3
vi	Test Data Preparation	1	4	2
vii	Test Executions and Defect Reporting for Functional Testing (Integration Testing, Smoke Testing, System Testing and Regression Testing)			
viii	Test Executions and Defect Reporting for Non-Functional Testing (Performance Testing, Load Testing, Stress Testing and Security Testing)			3
ix	Test Summary	1	2	2
	Total	4	13	18
	*Note: - Please see Column 5 of Table 1 of Note I for the definition of “working day”.			

Note IV: Standards for Cyber Security

A **security audit** is the high-level description of the many ways organizations can test and assess **their** overall **security** posture, including cybersecurity. The objective of audit is to understand, address and manage the cyber security risks and improve the security posture in all AP Government organizations in a cost-effective manner. The departments should ensure that the applications developed should be Security Audited and SSL/TLS certified before going Live.

All secretariat departments/HoDs/PSUs /Societies and Institutional entities under GoAP shall request Andhra Pradesh Technology Services (APTS) or any CERT-in empanelled organization for security audit, and SSL / TLS certification.

Form A - Online Indent Form for Organizational On-boarding for Data Access through API*

Sl. No.	Information requested on	Response of department
1.	Name and address of Organization	
2.	State the Purpose of Data API* usage	
3.	Has the requesting department integrated with the URL of the data source?	
4.	Is the URL of the data source audited? (If the response is “yes”, upload a valid security audit certificate. If response is “no”, data sharing and access must be denied)	
5.	- Is the requesting API integrated with multiple applications (meaning, will the data be shared by multiple applications)? This is not efficient, may lead to misuse, and not permitted. - If yes, provide details.	
6	Give details of the application for which the data is proposed to be used.	
7	Period for which the data access and sharing is requested	
8	Email and contact details of the SPOC** in the requesting department	
9	Email and contact details of the government official, responsible for the application from the requesting department	
10	Competent Authority to Approve the data request in the source entity	
11	Approval from the Competent Authority with remarks	

* API stands for application programming interface

**SPOC stands for the single point of contact

Process work flow:

1. Online Indent form will be made available as above
2. The requesting department must fill the form online, ensure authentication by the requesting HoD, and uploaded on the portal of the requesting department, thereby ensuring date and time stamp, and audit trails
3. The application goes in work flow of data donor, checks the API etc
4. Data shall be accessed, and shared by the requesting department only after the Competent Authority in the source department grants the approval in the online indent form. The approved online indent form must also be uploaded on the portal of the requesting and the source department.
5. The source department must maintain a detailed log online of the requests, with unique request IDs and the sharing date-wise. This detailed log shall be shared by the source departments with all the requesting departments on a monthly basis.

Table 3: Details of data of e-Government applications shared through Application Programming Interface (APIs)

(To be filled-in by the Department/ HoD which shared the data)

S.No	Date of data share	Purpose, and size of data shared	Name, email id, and contact details of the person/ organization with whom data was shared	Period for which the data access and sharing was requested	Name, email, and contact details of official who authorized the data share
1					
2					
3					

Table 4: Details of data of e-Government applications shared through insecure protocols

(To be filled-in by the Department/ HoD which shared the data)

S.No	Data uploaded over	Date of data share	Purpose, and size of data shared	Name, email id, and contact details of the person / organization with whom data was shared	Period for which the data access and sharing was requested	Name, email, and contact details of official who authorized the data share
1	Hyper Text Transfer Protocol (http)					
2	Webmail					

3	File transfer Protocol (FTP)					
4.	Peer-to-Peer (P2P)					
5.	Other insecure sources					

Useful Links and References:

1. https://meity.gov.in/writereaddata/files/Approved%20Social%20Media%20Frame%20work%20and%20Guidelines%20_2_.pdf. [Reference for the Compliance reports on the standards for Social Media Accounting for Government Organizations]
2. ¹<https://cmminstitute.com/learning/appraisals/levels> [Reference used for preparing the Compliance reports on the standards for the CMMI level definitions to be possessed by the Vendor who are supporting the Departments for Development, Integration, Data Hosting, Website development and Mobile Application Development]
3. URL:<https://ITAssets.apts.gov.in>. [Reference used for mandating all the Government Departments to take the ownership of securing the Critical Information Infrastructure (CII), (IT infrastructure, Websites, Web and Mobile applications, etc.). The details of CII should be entered in this website created by APTS]
4. Cyber Security Frame Work – [GOMs.No.18, Dated:06.03.2019 of ITE&C Department, Andhra Pradesh Cyber Security Frame work (APCSF) – for effective implementation of the ‘AP Cyber Security Policy 2017’ across the state]. [Reference for preparing the Compliance reports on the standards for Cyber Security for the Government applications]
5. Cyber Security Policy - [GOMs.No.2, Dated:01.03.2017 of ITE&C Department, Andhra Pradesh Cyber Security Policy 2017]. [Reference used in for preparing the Compliance reports on the standards for Cyber Security for the Government applications]
6. Cyber Security Assurance services-[GOMs.No.4, Dated:10.01.2019 of ITE&C Department, Andhra Pradesh Cyber Security Frame work (APCSP) 2017– for Cyber Assurance Services by Nodal Agency –Critical Information Infrastructure to undergo Mandatory Audits by all secretariat Departments/HoDs/PSUs/Societies and Institutions]. [Reference used for preparing the Compliance reports on the standards for Cyber Security for the Government applications]
7. Cyber Security Operations Centre. [GOMs.6, Dated:25.01.2019 of IT, E&C Department – Andhra Pradesh Cyber Security Policy (APCSP) 2017 – Andhra Pradesh Cyber Security Operations Centre (APCSOC) – Onboarding IT Assets by all Secretariat Departments/ HoDs/ PSUs/ Societies and Institutions with APCSOC]

for continuous IT Security monitoring.[Reference used in for preparing the Compliance reports on the standards for Cyber Security of the Government applications]

8. Web Security Guidelines by NIC Computer Emergency Response Team(CERT), released in November 2017. ([https:// nic - cert.nic.in / pdf / Website % 20Security % 20Guidelines.pdf](https://nic-cert.nic.in/pdf/Website%20Security%20Guidelines.pdf))[Reference used for preparing the Compliance reports on the standards for web security of Government applications]
9. https://web.guidelines.gov.in/assets/documents/pdf/hand_book.pdf. [Reference used for preparing the Compliance reports on the standards for Data Hosting of Government applications]
10. <http://egovstandards.gov.in/sites/default/files/GOI%20Web%20Guidelines.pdf>. [Reference used for preparing the Compliance reports on the standards for web site development]
11. https://dot.gov.in/sites/default/files/2018_06_21%20Endorsement%20GIGW%20Ed%20to%20DoT%20Units.pdf. [Reference used for preparing the Compliance reports on the standards for the Mobile Applications of the Government applications]
12. https://web.guidelines.gov.in/assets/documents/pdf/hand_book.pdf. [Reference used for preparing the Compliance reports on the standards for Standard Testing and Quality Control of the Government applications]
13. <https://in.pcmag.com>. [Reference used for identifying Antivirus software as ranked by one of the popular industry magazines]
14. <https://www.cyberoam.com/layer8.html> [Reference used for the compliance matrix on the standards for Data sharing and Data base access where the Cyberoam Layer 8 Technology, a contemporary cybersecurity paradigm, adds over its network security appliances the user identity, which is the 8th layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username]

[1] <https://cmmiinstitute.com/learning/appraisals/levels> accessed on 20-6-2020

[2] Cyberoam Layer 8 Technology, a contemporary cyber security paradigm, adds over its network security appliances treat user identity the 8th layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username. See <https://www.cyberoam.com/layer8.html> accessed on 20-6-2020

[3] For example, with reference to the ITE&C department, the “national portal” is <https://meity.gov.in/>

[4] See <https://cmmiinstitute.com/learning/appraisals/levels> accessed on 20-6-2020
